Appendix F
Executive Summaries

This IATF section is a repository for Executive Summaries. An Executive Summary captures the essence of a user's need in clear, concise statements. The security approach outlined in the Executive Summary points to supporting documentation such as protection profiles.

The Target Environment section describes the purpose and scope of the executive summary and associated protection profiles. It includes the following:

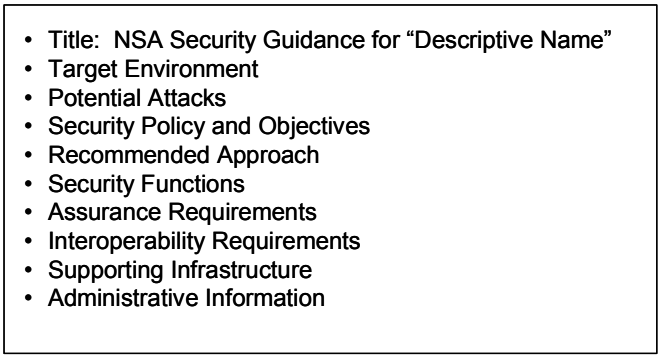

Figure F-1. Executive Summary Outline

- Which kind of Protection Profile (PP) is this (e.g., defense-in-depth, technology goal, customer-specific)?
- Describe the types of user organizations in the scope of this document.
- What does the user organization want the system to do?
  - What is the problem the system is intending to solve?
- Summarize the system environment:
  - Where does the system operate?
  - How will the system be used?
  - Provide a diagram of the system context.

The Potential Attacks section includes the following:

- What are the information system attacks/events for which protection is needed?
  - How can an adversary harm the user organization's mission by attacking the system?
  - What nonmalicious events (e.g., flood, user error) can harm the user organization's mission through information system effects?
- Attacks should be relevant to the technology under consideration, but should not assume implementation details.

The Security Policy and Objectives section includes the following:

- What is the organization policy or other rules that the system must meet or support?
  - Provide the technology-unique context for the policy and objectives (e.g., defend-the-enclave, tunneling).

  - Referencing Global Information Grid (GIG) policy, describe the robustness category (basic, medium, or high) and any recommended deviations from the policy.

- Describe the level of threat and value of information.
- What are the information domains of interest?
  - An information domain is defined by a *type of information* and the *set of users* with *specific privileges* for access to that information.
- What security objectives must the system meet to protect against the information system attacks?

The Recommended Approach section includes the following:

- What is the conceptual architecture for the system?
- Which security functions are allocated to the technology under consideration?
- What are the dependencies on security functions of other system components?
- Diagram of the system should be included.

The Security Functions Section includes the following.

- What are the security functional requirements for the system?
  - Include strength of mechanisms and cryptographic algorithm suite.
- What security services must the system perform for each information domain (e.g., confidentiality, integrity, and availability)?
- Describe compliance with GIG policy for placement of security functions.

The Assurance Requirements section includes the following:

- Indicate the required Evaluated Assurance Level (EAL) as defined in the Common Criteria.
- Describe additional assurance requirements or (e.g., Federal Information Processing Standard [FIPS] 140-1 verification).
- Describe compliance with GIG policy for assurance.

Interoperability Requirements section includes the following:

- What are the interoperability requirements that the system components must meet? (e.g., Transmission Control Protocol [TCP]/Internet Protocol [IP], security protocols).

The Supporting Infrastructure section includes the following:

- What support does the system require from key management infrastructure (e.g., certificate class and version)?

- What support does the system require from network security management infrastructure (e.g., audit analysis)?

The Administrative Information section of each Executive Summary must include the following:

- List of PPs within the scope of the Executive Summary.
- Date and version number.
- Author block.
- Approval block.

The National Security Agency (NSA) will provide additional configuration management guidance.

This page intentionally left blank.